ROUTING AND RECORD SHEET

SUBJECT: (Optional)

Personnel Security Committee Meeting

FROM: | **EXTENSION** | **NO.**

25X1

DATE

TO: (Officer designation, room number, and building)	DATE RECEIVED	DATE FORWARDED	OFFICER'S INITIALS	COMMENTS (Number each comment to show from whom to whom. Draw a line across column after each comment.)
1. C/POL. BR.	6/11/87		[illegible]	
2. EO	6/12/87		[illegible]	
3. D/S			[illegible]	
4. OS/Registry				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				

25X1

FORM 1-79 **610** USE PREVIOUS EDITIONS

☆ U.S. Government Printing Office: 1985—494-834/49156

Personnel Security Committee
Washington, D.C. 20505

12 JUN 1987

MEMORANDUM FOR: Distribution

FROM: [redacted] 25X1
Chairman, Personnel Security Committee

SUBJECT: Personnel Security Committee Meeting

1. The Personnel Security Committee (PSC) will meet on Tuesday, 23 June 1987, from 1000-1130 hours in Room 6W02, [redacted] 25X1
Washington, D.C.

2. Among those tasks detailed in Attachment A are items, principally from the SSCI report, which the C/IG/CM(P) suggests might be assigned to the PSC. Attachment B lists tasks assigned to the IG/CM(P) but with no recommended assignment. Members are asked to be prepared to discuss the tasks of interest to your agency or department.

3. On 19 June, the chairmen of the committees under the IG/CM(P) will meet to take a preliminary cut at these issues. I will report the results to you on 23 June.

4. Members and alternates who have attended previous meetings need not recertify their clearances; however, new attendees should provide their names, social security numbers, and clearances by 19 June to [redacted] 25X1 25X1

OS 7 2159/A

Unclassified when separated from
SECRET attachment

S E C R E T

SUBJECT: Personnel Security Committee Meeting

OS/EO/PPS/JWM/ [redacted] (11 Jun. 87) STAT

Distribution of OS 7 2159 (w/att as shown):

1 - Mr. Major, NSC
1 - Mr. Donnelly, DOD
1 - Mr. Garcia, OPM
1 - Col. Gallo, ARMY
1 - Mr. Allen, OPNAVSSO
1 - Mr. Cornett, USAF
1 - Capt. Carter, MARINE CORPS
1 - Mr. O'Donnell, TREASURY
1 - Mr. Seaton, ENERGY
1 - Mr. Dittmer, STATE
1 - Mr. Stoops, FBI
1 - [redacted] STAT
1 - [redacted] STAT
1 - Mr. Rubino, JUSTICE
1 - Mr. Turner, COMMERCE
1 - Mr. Garfinkel, ISOO
1 - [redacted] STAT
1 - OS/Registry
1 - PPS Chrono
1 - D/S Chrono

UNCLASSIFIED

A

ATTACHMENT C

GROUP I ISSUES

Assigned to an IG/CM(P) committee, but no status report received as of 8 May 1987:

D. IMPROVE MANAGEMENT

1. Review the Stilwell Commission proposals on managing and controlling classified information for possible government-wide implementation. [redacted] 25X1

P. 337, SSCI report (Item 81). Lead: Information Security Committee (ISC)

6. Change the Federal Acquisition Regulations to designate industrial security for classified contracts as a direct cost. The primary intent of this proposal is to identify and monitor security costs associated with particular contracts. [redacted] 25X1

P. 344, SSCI report (Item 108). Lead: ISC

7. Consideration should be given to greater use of Cost Plus Award Fee contracts as an incentive for fulfilling contract security requirement. [redacted] 25X1

P. 344, SSCI report (Item 109). Lead: ISC

8. Require trained and government-certified security officers in each classified contract, including those for special access programs. [redacted] 25X1

P. 344, SSCI report (Item 110). Lead: ISC

II. SAFEGUARD INFORMATION WHOSE UNAUTHORIZED DISCLOSURE COULD JEOPARDIZE US NATIONAL SECURITY

B. IMPROVING INFORMATION SECURITY

3.b. Modify Executive Order 12356 to require greater controls on special access programs and to give the ISOO Director greater

[redacted] 25X1

SECRET

authority to oversee such programs. The Secretary of Defense should have sole authority to approve defense-related, non-intelligence special access programs. The whole government should conduct a comprehensive review and revalidation of all existing special access programs and associated "carve out" contracts, with an independent assessment by the ISOO Director. Such reviews should be repeated on a periodic basis. [redacted] 25X1

P. 337, SSCI report (Item 82). Lead: ISC

4.a. Expand the ISOO's staff to include a permanent inspection element. ISOO should work with DIS to implement improved training courses on information security and classification management. ISOO and the DCI should also reassess special markings with a view to simplification. ISOO should ensure that agencies designate individuals/positions with responsibility for determining need-to-know access. [redacted] 25X1

P. 337, SSCI report (Item 83). Lead: ISOO/ISC

4.b. Make the formulation of "need-to-know" limitations and procedures an integral part of the development process for new or improved technical collection systems, with plans and costs included in budget proposals for such systems. The Community should also devote increased effort to planning and training for war-fighting situations in which dissemination limits will have to be substantially reduced. [redacted] 25X1

P. 337, SSCI report (Item 84). Lead: ISOO/ISC

5. Other Harper Committee recommendations approved by DoD should be implemented promptly and reviewed for government-wide application. [redacted] 25X1

P. 344, SSCI report (Item 112). Lead: ISC

7.b. Consider simplifying the classification system by establishing two levels, eliminating the current Confidential classification. This streamlining should be preceded by consultation with other countries with whom the United States shares security classification agreements. [redacted] 25X1

P. 336, SSCI report (Item 79). Lead: ISC

8. Ensure implementation of the Stilwell Commission recommendations on National Disclosure Policy not only for military information, but for sensitive intelligence and nuclear matters as well. [redacted] 25X1

P. 344, SSCI report (Item 111). Lead: OSD-State-DoE/ISC

11.e. Promulgate an executive order requiring each agency to establish procedures governing authorized disclosure of classified information to the news media, including background disclosures of information that remains classified. Such procedures should require records for accountability, consultation with originating agencies, and designation of officials authorized to disclose classified information to the media. [ ] 25X1

P. 336, SSCI report (Item 80). Lead: ISC

12. Consider postponement of new criminal penalties for unauthorized disclosure until after the appeals in the Morison case. The Committee supports continued internal agency and FBI investigations for purposes of administrative discipline as well as prosecution, including use of voluntary polygraph examinations under criminal investigative procedures. DoJ guidelines for leak investigations should be revised to reflect current policy of using administrative sanctions when prosecution is not pursued. [ ] 25X1

P. 338, SSCI report (Item 85). Lead: DoJ/ISC

C. UPGRADING PERSONNEL SECURITY

1.b. Issue a new Executive Order on personnel security. The order should provide for government-wide minimum standards and procedures and a policy oversight office similar to the Information Security Oversight Office. It should focus exclusively on personnel security programs regarding access to classified information and to sites where classified information is maintained. Drafting of this order should not delay action on other recommendations. [ ] 25X1

P.334, SSCI report (Item 71). Lead: PSC

2. Establish a national crypto-access program and a similar program for that group of individuals requiring extensive access to major automated information systems processing classified information or any continuing access to specially sensitive systems. [ ] 25X1

P. 27, President's report. Lead: NSA-CIA/PSC

5.c. Increase personnel security research, including expanded research and evaluation on the wider use of psychological testing in the clearance process, taking full account of individual rights, as well as the implications of recent espionage cases. [ ] 25X1

PP. 333-334, SSCI report (Item 70). Lead: PSC

5.d. Improve the adjudication process for granting or denying security clearances, with more rigorous standards regarding persons who have committed felony offenses; follow-up measures where persons with admitted problems like drug use are cleared; and a government-wide requirement for training of adjudicators. For the most sensitive positions, a "select in" policy based on demonstrated aptitude for security should be adopted in place of the current "select out" policy based on the absence of proved disqualifying factors. [redacted] 25X1

P. 334, SSCI report (Item 72). Lead: PSC

6.a. Reach agreement on a "single scope" background investigation for all Top Secret and SCI clearances. The uniform policy should provide for: (a) less costly and more timely background investigations and clearances; (b) highest priority for meeting the five-year reinvestigation requirement; and (c) a subject interview in all cases. [redacted] 25X1

P.332, SSCI report (Item 64). Lead: OSD-CIA-NSA/PSC

6.b. Postpone implementation of the proposal for one-time, short duration access by cleared personnel to the next higher level of classified information until Secret clearance requirements and investigations are upgraded and the IG/CM(P) has reviewed the issue. [redacted] 25X1

P. 333, SSCI report (Item 68). Lead: PSC

7. Ensure substantially increased funding for personnel security in all relevant departments and agencies. A government-wide plan should be submitted to Congress to achieve the following goals: (a) elimination of the reinvestigation backlog for Top Secret (including SCI) within four years: and (b) implementation within less than ten years of a program for intensified investigation and reinvestigation for Secret clearances. [redacted] 25X1

P. 332, SSCI report (Item 63). Lead: OSD-CIA-NSA/PSC

8. Establish government-wide standards for the use of contractors to conduct personnel field investigations, including requirements for supervision and quality control, restrictions on use of information, exclusion of contractors from adjudication decisions, and standards for experimentation with new procedures for less sensitive clearances. [redacted] 25X1

P. 332, SSCI report (Item 65). Lead: PSC

9.a. Consider government-wide adoption of the Stilwell Commission recommendations to prohibit the practice of requesting security clearances solely to provide access to a controlled area, where there is no need to know or even to be exposed to classified information. Reliability investigations should still be conducted in such cases, with standards equal to those proposed by this report for Secret clearances. [redacted] 25X1

P. 333, SSCI report (Item 66). Lead: PSC

9.b. Reduce the number of clearances held by industry. The DoD goal of a ten percent reduction in FY 1986 should be applied by the DCI (for SCI programs) and the Secretary of Energy. ([redacted] 25X1

P. 344, SSCI report (Item 107). Lead: ISC

10.a. Establish more effective means for investigating and clearing immigrant aliens and foreign nationals overseas who are granted access to classified information. [redacted] 25X1

P. 333, SSCI report (Item 67). Lead: PSC

10.b. Ensure full coordination of departmental policies and practices for the use of polygraphing in personnel security screening, to maintain stringent quality controls and safeguards for individual rights, to prevent over-reliance on this technique, to provide for necessary research and funding, and to improve understanding of the procedures. [redacted] 25X1

P. 335, SSCI report (Item 74). Lead: PSC

11. Initiate a pilot program for assignment of DIS personnel to large sensitive contractor facilities on a full-time basis, and the results should be reviewed as a basis for similar government-wide practice. [redacted] 25X1

P. 343, SSCI report (Item 105). Lead: ISC

D. IMPROVING OPERATIONS SECURITY

2. Conduct an overall review of the alerting systems (for example, SATRAN) that provide warning of overflights by air and space platforms to determine the adequacy and effectiveness of such systems. [redacted] 25X1

P. 25, President's report. Lead: DoD/NOAC

4. Develop government-wide operations security (OPSEC) objectives and ensure that relevant agencies have the necessary resources and programs to achieve those goals. [redacted] 25X1

P. 331, SSCI report (Item 61). Lead: NOAC

B

GROUP II ISSUES

To be undertaken by an ad hoc working group on the IG/CM(P), but no action undertaken as of 8 May 1987:

I. ENHANCE PROFESSIONALISM OF THE WORK FORCE

B. IMPROVE TRAINING

1. Make the adequacy of security training an item of recurring interest for agency Inspectors General. [redacted] 25X1

   P. 18, President's report. Lead: IG/CM(P)-Work Group (WG)

2. Consider phased assignment of national responsibilities for security training to the Defense Security Institute, with an interagency group including representatives from US counterintelligence agencies to develop security awareness materials and with a West Coast annex. [redacted] 25X1

   P. 331, SSCI report (Item 60). Lead: OSD-IG/CM(P)-WG

3. Establish government-wide security training objectives and require minimum levels of training and certification for industrial security officers, clearance adjudicators, and other positions requiring consistent standards. [redacted] 25X1

   P. 331, SSCI report (Item 59). Lead: IG/CM(P)-WG

C. INCREASE SECURITY AWARENESS

3. Strengthen interagency procedures for bringing possible espionage cases to the FBI's attention in a timely manner. The FBI should also be informed when employees with access to extremely sensitive information, such as Howard and Pelton, resign or are dismissed under circumstances indicating potential motivations for espionage. [redacted] 25X1

   P. 316, SSCI report (Item 13). Lead: IG/CM(P)-WG

D. IMPROVE MANAGEMENT

2. Emphasize commander and manager responsibility for security, including government-wide application of the recent DoD action to incorporate security into performance evaluations and development of more realistic and consistent policies for disciplinary sanctions. [redacted] 25X1

P. 330, SSCI report (Item 57). Lead: OSD-IG/CM(P)-WG

3. Assess requirements for research and analysis on security countermeasures to promote aggressive and balanced efforts government-wide, especially on personnel security. [redacted] 25X1

P. 330, SSCI report (Item 56). Lead: IG/CM(P)-WG

4. Enhance security policy and oversight capabilities in the Office of the Secretary of Defense so as to ensure integration of policies for the various DoD security programs. [redacted] 25X1

P. 329, SSCI report (Item 54). Lead: OSD-IG/CM(P)

9. Evaluate security countermeasures resource priorities for the NSC and OMB on an annual basis. Security resources should be identified by function and program in departmental and agency budget justifications. The administration and the Congress should consider additional ways to implement a more coherent budget process for security programs. [redacted] 25X1

P. 330, SSCI report (Item 55). Lead: IG/CM(P)/Work Group (WG)

II. SAFEGUARD INFORMATION WHOSE UNAUTHORIZED DISCLOSURE COULD JEOPARDIZE US NATIONAL SECURITY

C. UPGRADING PERSONNEL SECURITY

4. Vigorously implement the other Stilwell Commission recommendations on personnel security in DoD with augmented OSD policy oversight, and review them at the NSC level for adoption government-wide. [redacted] 25X1

P. 335, SSCI report (Item 76). Lead: OSD-IG/CM(P)-Work Group